STATE OF VERMONT
Agency of Administration

STANDARD **STC** **State Technology Collaborative**	**ORIGINAL POLICY ADOPTED BY STC** **DATE:**	**ORIGINAL POLICY NUMBER**
	EFFECTIVE DATE	**ASSOCIATED DOCUMENTS** Data Encryption Policy Data Protection Policy Password Policy Password Standard

STATUTORY REFERENCE OR OTHER AUTHORITY: Personnel Policies and Procedures
ELECTRONIC COMMUNICATIONS AND INTERNET USE -
http://www.State.vt.us/pers/er/pm/pm117.htm

APPROVAL DATE:

APPROVED BY: Secretary of Administration

STANDARD TITLE: Data Encryption for Laptops and Tablet Computers

STANDARD STATEMENT: As governed by the State of Vermont Data Encryption Policy, this document identifies the State's current **standards and best practices** for encrypting confidential information as defined in the accompanying policy, contained on laptops and mobile devices. Data Encryption includes the safeguards and preventative measures taken to:

- Guard confidential data against malicious intent, unauthorized access, modification or loss.

STANDARDS FOR DATA ENCRYPTION

1.1 Confidential Data on all laptops and tablet computers shall be encrypted. Confidential Data includes but is not limited to social security numbers, personal financial information, debit/credit card numbers, personally identifiable health information, and any other data that is identified by law, regulation, policy, or practice as confidential. Agencies and Departments are required to identify any additional Confidential Data specific to their business practices that warrants the protection of encryption.

1.2 Encryption keys used to encrypt data must not be stored with or on the device. Agency and/or departmental IT staff must retain a “master key” and establish a key management process for access to the data should the employee lose his or her key.

1.3 Data shall be encrypted with algorithms utilizing a key length of 128 bits or longer.

1.4 Acceptable encryption methods employ a user-specified password to generate an encrypted output, called cipher text, in such a way that, given the cipher text, it is extremely difficult to recover the original plaintext without the encryption password in a reasonable amount of time. The algorithms that combine the keys and plaintext that are acceptable fall in one of the three following categories include, *but are not limited to:*

1.4.1 Block Cipher
1.4.2 Stream Cipher
1.4.3 Hash Algorithms

1.5 Unacceptable encryption methods include, *but are not limited to:*
1.5.1 DES (Data Encryption Standard)
1.5.2 Wired Equivalent Privacy (WEP)

BEST PRACTICE FOR DATA ENCRYPTION

2.1 For devices without Confidential Data, Microsoft Windows native encryption is suggested as a measure to protect data.
2.2 Examples of acceptable encryption methods include, but are not limited to:

2...2.1 Triple-DES
2.2.2 Advanced Encryption Standard
2.2.3 International Data Encryption Algorithm (IDEA)
2.2.4 RSA
2.2.5 ElGamal
2.2.6 SSL (secure socket layer) v3
2.2.7 PGP

2.3 While this policy is specific to laptop and tablet computers, all users, Agencies, and Departments should deploy encryption for portable media or storage devices, such as thumb drives, flash drives, zip drives, CD’s, DVD’s, MP3, floppy disks or any device that contains Confidential Data that can easily be carried out of the workplace, and must comply with all statutes, regulations, or policies that require such encryption.

2.4 Agencies and Departments should consider encrypting all laptops, tablets and portable devices.